

# Lista zadań – wdrożenie reformy ochrony danych osobowych wprowadzonej przez RODO

**dr Marlena Sakowska-Baryła**

radca prawny

Sakowska-Baryła, Czaplińska

Kancelaria Radców Prawnych Sp.p.



## Podstawa prawna

- art. 47 i art. 51 Konstytucji RP z 02.04.1997 r.
- **Ustawa z dnia 29.08.1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922) – dalej uodo**
- **Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)**  
**Dz.U.UE.L.2016.119.1; dalej: rodo, *stosowane od 25 maja 2018 r.***

**Projekty z 12.09.2017 r. ustawy o ochronie danych osobowych oraz ustawy przepisy wprowadzające ustawę o ochronie danych osobowych:**

[https://mc.gov.pl/files/ustawa\\_o\\_ochronie\\_danych\\_osobowych\\_-\\_projekt\\_-\\_13.09.2017.pdf](https://mc.gov.pl/files/ustawa_o_ochronie_danych_osobowych_-_projekt_-_13.09.2017.pdf)

[https://www.mc.gov.pl/files/ustawa\\_-\\_](https://www.mc.gov.pl/files/ustawa_-_)

[przepisy\\_wprowadzajace\\_ustawe\\_o\\_ochronie\\_danych\\_osobowych\\_-\\_13.09.2017.pdf](przepisy_wprowadzajace_ustawe_o_ochronie_danych_osobowych_-_13.09.2017.pdf)

## Ustalenie w jakiej roli występuje organizacja

administrator

współadministrator

procesor

subprocesor

# rodo

## Artykuł 4. pkt 7

"**administrator**" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który **samodzielnie lub wspólnie z innymi** ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

**współadministrator**

## RODO: Artykuł 26. Współadministratorzy

### 1. **Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami.**

W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z niniejszego rozporządzenia, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.

## RODO: Artykuł 26. Współadministratorzy

2. Uzgodnienia, o których mowa w ust. 1, należycie **odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą.** Zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą.
3. **Niezależnie od uzgodnień, o których mowa w ust. 1,** osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z niniejszego rozporządzenia **wobec każdego z administratorów.**

## Artykuł 4

**8) "podmiot przetwarzający"** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

## Artykuł 28 Podmiot przetwarzający

1. Jeżeli przetwarzanie ma być dokonywane **w imieniu administratora**, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.

Podmiot przetwarzający —————> subprocesor

**Podpowierzenie:**

2. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian

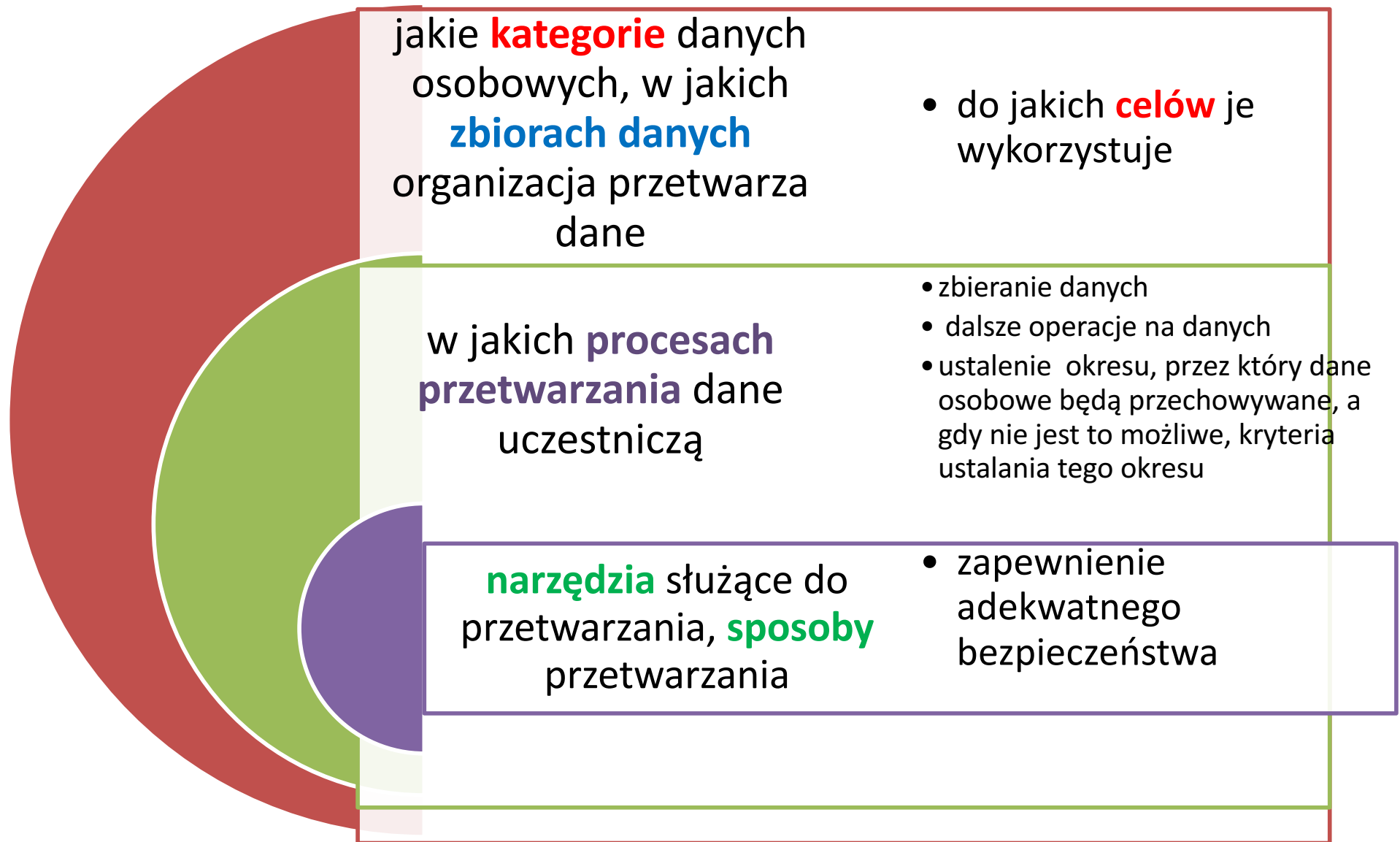
subprocesor



## Podpowierzenie

4. Jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają - na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego - **te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym**, o których to obowiązkach mowa w ust. 3, w szczególności obowiązków zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.

# Ustalenie zasobów



# „dane osobowe” w rodo

## Art. 4 pkt 1 rodo

**"dane osobowe"** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

## „dane zwykłe” i „dane wrażliwe”

Zabrania się przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym (art. 27 ust. 1 uodo)

„dane wrażliwe” → szczególne kategorie danych osobowych  
(motyw 10)

## Art. 9 rodo

### Przetwarzanie **szczególnych kategorii danych osobowych**

1. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

„dane wrażliwe” → dane dotyczące wyroków skazujących i naruszeń prawa

## Art. 10 rodo

### Przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa

Przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa **na podstawie art. 6 ust. 1** wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych.

# pseudonimizacja

## Artykuł 4

5) "**pseudonimizacja**" oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

## Artykuł 4

- 13) "dane genetyczne"** oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
- 14) "dane biometryczne"** oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
- 15) "dane dotyczące zdrowia"** oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia;



## RODO: Przetwarzanie danych

### Artykuł 4

- 2) "przetwarzanie"** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
- 3) "ograniczenie przetwarzania"** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

## RODO: Profilowanie

### Artykuł 4

**4) "profilowanie"** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

# RODO: Zbiór danych

## Artykuł 4

**6) "zbiór danych"** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

## Artykuł 2 **Materialny zakres stosowania**

1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych **w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.**

## Ustalenie zasobów

- **Działania inwentaryzacyjne** – punkt wyjścia do przeprowadzenia analizy wpływu RODO na prowadzoną działalność.
- Pozwala organizacji, jeszcze **przed zaangażowaniem się w znaczne wydatki**, zrozumieć jakie prace należy wykonać by skutecznie zrealizować projekt.
- **Analiza wpływu RODO na prowadzoną działalność** to materiał, który pozwala zbudować pełną świadomość u osób decyzyjnych i zapewnić niezbędne zasoby, tj. ludzi i budżet do przeprowadzenia projektu.

## Przegląd procesów przetwarzania

- **przegląd procesów przetwarzania danych pod kątem zasad przetwarzania z RODO (art. 5)** - zgodności z prawem, rzetelności, przejrzystości, celowości, minimalizacji danych, ograniczenia czasowego, prawidłowości, integralności, poufności



rozliczalność

## Artykuł 5. Zasady dotyczące przetwarzania danych osobowych

1. Dane osobowe muszą być:

- a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("**zgodność z prawem, rzetelność i przejrzystość**");
- b) zbierane w konkretnych, wyraźnych i **prawnie uzasadnionych celach** i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami ("**ograniczenie celu**");
- c) adekwatne, stosowne oraz ograniczone do tego, co **niezbędne do celów**, w których są przetwarzane ("**minimalizacja danych**");
- d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("**prawidłowość**");

## Artykuł 5. Zasady dotyczące przetwarzania danych osobowych

- e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą ("**ograniczenie przechowywania**");
- f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("**integralność i poufność**").

**2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie ("**rozliczalność**").**

## Przegląd procesów przetwarzania

- **Zidentyfikowanie i analiza procesów przetwarzania danych, objętych dodatkowymi restrykcjami co do legalności.**
- Prywatność w fazie projektowania
- Domyślna ochrona danych
- Szacowanie ryzyka
- Ocena skutków dla ochrony danych
- Wyróżniamy procesy, w których odbywa się podejmowanie decyzji opartych na zautomatyzowanym przetwarzaniu, w tym profilowanie, przetwarzanie szczególnych kategorii danych osobowych czy danych osobowych dzieci, w przypadku oferowania im usług społeczeństwa informacyjnego.



# RODO

## Artykuł 25 Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz **ryzyko** naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator - zarówno **przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania - wdraża odpowiednie środki techniczne i organizacyjne**, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

# RODO

## Artykuł 25 Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, **aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.** Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.
3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 i 2 niniejszego artykułu, można wykazać między innymi poprzez wprowadzenie zatwierdzonego mechanizmu certyfikacji określonego w art. 42.

# RODO

## Artykuł 24 Obowiązki administratora

1. Uwzględniając **charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia** praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża **odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać.** Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
2. Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora **odpowiednich polityk** ochrony danych.
3. Stosowanie zatwierdzonych kodeksów postępowania, o których mowa w art. 40, lub zatwierzonego mechanizmu certyfikacji, o którym mowa w art. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciężących na nim obowiązków.

## Legalność przetwarzania danych

w rodo określono przypadki, kiedy przetwarzanie danych jest dopuszczalne – przesłanki dopuszczalności przetwarzania

przypadki te są od siebie niezależne – wystarczy, jeśli przetwarzanie danych będzie miało oparcie w jednej z przesłanek

Nie zawsze przetwarzanie danych osobowych odbywa się na podstawie zgody na przetwarzanie danych

wybór przesłanki zależy od tego, czy mamy do czynienia z „danymi zwykłymi” czy z „danymi wrażliwymi”

### Artykuł 6. Zgodność przetwarzania z prawem

1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - **spełniony jest co najmniej jeden z poniższych warunków:**
  - a) osoba, której dane dotyczą wyraziła **zgode** na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
  - b) przetwarzanie jest niezbędne do **wykonania umowy**, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
  - c) przetwarzanie jest niezbędne do wypełnienia **obowiązku prawnego ciążącego na administratorze**;
  - d) przetwarzanie jest niezbędne do **ochrony żywotnych interesów osoby**, której dane dotyczą, lub innej osoby fizycznej;

## Rodo – rozdział II ZASADY

### Artykuł 6. Zgodność przetwarzania z prawem

1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - **spełniony jest co najmniej jeden z poniższych warunków:**
  - e) przetwarzanie jest niezbędne do **wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;**
  - f) **przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów** realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

**Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.**

## Rodo: przetwarzanie szczególnych kategorii danych

### art. 9 ust. 2

Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:

- a) osoba, której dane dotyczą, wyraziła **wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach**, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;
- b) przetwarzanie jest niezbędne do **wypełnienia obowiązków i wykonywania szczególnych praw** przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
- c) przetwarzanie jest niezbędne do **ochrony żywotnych interesów** osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;

- d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
- e) przetwarzanie dotyczy danych osobowych **w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;**
- f) przetwarzanie jest **niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;**
- g) przetwarzanie jest **niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego**, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;



- h)** przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub **medycyny** pracy, do oceny zdolności pracownika do pracy, diagnozy **medycznej**, zapewnienia **opieki zdrowotnej** lub **zabezpieczenia społecznego**, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;
- i)** przetwarzanie jest niezbędne ze względów związanych z interesem publicznym **w dziedzinie zdrowia publicznego**, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
- j)** przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych **zgodnie** z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

## Ocena skutków dla ochrony danych

**Motyw 85:** Aby poprawić przestrzeganie niniejszego rozporządzenia, **gdy operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych**, należy zobowiązać administratora do dokonania oceny skutków dla ochrony danych w celu oszacowania w szczególności **źródła, charakteru, specyfiki i powagi tego ryzyka**. Wyniki oceny należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z niniejszym rozporządzeniem. Jeżeli ocena skutków dla ochrony danych wykaże, że operacje przetwarzania powodują **wysokie ryzyko**, którego administrator nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia, przed przetwarzaniem należy skonsultować się z organem nadzorczym.

## Motyw 89

Dyrektywa 95/46/WE przewidywała ogólny obowiązek zawiadamiania organów nadzorczych o przetwarzaniu danych osobowych. Obowiązek ten powodując jednak obciążenia administracyjne i finansowe i nie zawsze przyczyniał się do poprawy ochrony danych osobowych. **Dlatego należy znieść te powszechne, ogólne obowiązki zawiadamiania i zastąpić je skutecznymi procedurami i mechanizmami koncentrującymi się w zamian na tych rodzajach operacji przetwarzania, które ze względu na swój charakter, zakres, kontekst i cele mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.** Takie rodzaje operacji przetwarzania obejmują w szczególności operacje, które wiążą się w szczególności z użyciem nowych technologii lub które są **nowe i nie zostały jeszcze poddane przez administratora ocenie skutków dla ochrony danych lub stały się niezbędne z uwagi na upływ czasu od pierwotnego przetwarzania.**

**OSOD składa się z etapów** – na podstawie  
zob. Mariola Więckowska, *Przewodnik po cenie  
skutków dla ochrony danych*, „ABI Expert” 2017,  
nr 1, s. 48-49

**Etap 1:** Wstępna ocena

**Etap 2:** Ocena skutków dla ochrony danych

**Etap 3:** Ocena ryzyka prywatności i rekomendowane  
środki zaradcze

**Etap 4:** Przygotowanie raportu końcowego

**Etap 5:** Monitoring wdrożenia

## RODO: Artykuł 35 Ocena skutków dla ochrony danych

1. Jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze **względu na swój charakter, zakres, kontekst i cele** z dużym prawdopodobieństwem może powodować **wysokie ryzyko** naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.
2. Dokonując oceny skutków dla ochrony danych, **administrator konsultuje się z inspektorem ochrony danych,** jeżeli został on wyznaczony.

## RODO: Artykuł 35 Ocena skutków dla ochrony danych

3. Ocena skutków dla ochrony danych, o której mowa w ust. 1, **jest wymagana w szczególności w przypadku:**
- a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
  - b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10; lub
  - c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

## RODO: Artykuł 35 Ocena skutków dla ochrony danych

4. **Organ nadzorczy ustanawia i podaje do publicznej wiadomości wykaz rodzajów operacji** przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych na mocy ust. 1. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych, o której mowa w art. 68.
5. **Organ nadzorczy może także ustanowić i podać do wiadomości publicznej wykaz rodzajów operacji przetwarzania niepodlegających wymogowi** dokonania oceny skutków dla ochrony danych. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych.
6. Jeżeli wykazy, o których mowa w ust. 4 i 5, obejmują czynności przetwarzania związane z oferowaniem towarów lub usług osobom, których dane dotyczą, lub z monitorowaniem ich zachowania w kilku państwach członkowskich lub mogące znacznie wpłynąć na swobodny przepływ danych osobowych w Unii, przed przyjęciem takich wykazów właściwy organ nadzorczy stosuje mechanizm spójności, o którym mowa w art. 63.

## RODO: Artykuł 35 Ocena skutków dla ochrony danych

### 7. Ocena zawiera co najmniej:

- a) **systematyczny opis planowanych operacji przetwarzania i celów przetwarzania**, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez administratora;
  - b) **ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne** w stosunku do celów;
  - c) **ocenę ryzyka** naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz
  - d) **środki planowane w celu zaradzenia ryzyku**, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.
8. **Oceniając** - w szczególności do celów oceny skutków dla ochrony danych - skutki operacji przetwarzania wykonywanych przez administratora lub podmiot przetwarzający, **uwzględnia się przestrzeganie przez takiego administratora lub taki podmiot przetwarzający zatwierdzonych kodeksów postępowania, o których mowa w art. 40.**



## RODO: Artykuł 35 Ocena skutków dla ochrony danych

9. W stosownych przypadkach administrator **zasięga opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania**, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania.
10. Ust. 1-7 nie mają zastosowania, jeżeli przetwarzanie na mocy art. 6 ust. 1 lit. c) lub e) ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej - chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych.
11. **W razie potrzeby, przynajmniej gdy zmienia się ryzyko** wynikające z operacji przetwarzania, administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.

## Przegląd klauzul

- ocena dotychczas stosowanych klauzul zgody pod kątem możliwości kontynuowania przetwarzania danych wg RODO.
- klauzule zgody należy zweryfikować i dostosować do warunków określonych w RODO we wszelkich procesach, gdzie dane pozyskiwane są na tej podstawie.

**Uwaga! Może to oznaczać aktualizację nie tylko papierowych i elektronicznych formularzy ale i skryptów rozmów, jeśli zgoda pozyskiwana jest telefonicznie.**

## Lista zadań

- **weryfikacja i dostosowanie umów powierzenia przetwarzania danych osobowych**.
- Zadanie to wiąże się z pracą prawników, w zakresie przygotowania nowej treści umowy/aneksów i angażuje również zespoły zakupowe, odpowiedzialne za kontakty z zewnętrznymi dostawcami, w zakresie renegocjowania kontraktów oraz może angażować właścicieli procesów biznesowych.

RODO: Artykuł 28 3. (...) Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

- a) przetwarza dane osobowe **wyłącznie na udokumentowane polecenie administratora** - co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej - chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;

## RODO: Artykuł 28 Podmiot przetwarzający

- b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
- c) podejmuje wszelkie środki wymagane na mocy art. 32;
- d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 4;
- e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III;
- f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32-36;

## RODO: Artykuł 28 Podmiot przetwarzający

- g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
- h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

W związku z obowiązkiem określonym w akapicie pierwszym lit. h) podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

## Przegląd klauzul

Przeładowi i zmianie poddajemy klauzule informacyjne przy zbieraniu danych .

Ich treść z pewnością ulegnie rozszerzeniu i może mieć bardziej opisowy charakter (art. 13 i art. 14 RODO)

## Realizacja praw osób, których dane dotyczą

- **Zaplanowanie obsługi wniosków w zakresie realizacji praw osób, których dane dotyczą,** w szczególności prawa dostępu do danych, ograniczenia przetwarzania, usunięcia, przenoszenia danych, prawa wniesienia sprzeciwu wobec przetwarzania danych osobowych na potrzeby marketingu, w tym profilowania.

**Przeszkolenie osób przyjmujących i realizujących wnioski podmiotów danych.**



## Rodo - ROZDZIAŁ III Prawa osoby, której dane dotyczą

- Artykuł 12 - Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą
- Artykuł 13 - Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą
- Artykuł 14 - Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą
- Artykuł 15 - Prawo dostępu przysługujące osobie, której dane dotyczą
- Artykuł 16 - Prawo do sprostowania danych
- Artykuł 17 - Prawo do usunięcia danych ("prawo do bycia zapomnianym")
- Artykuł 18 - Prawo do ograniczenia przetwarzania
- Artykuł 19 - Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania
- Artykuł 20 - Prawo do przenoszenia danych
- Artykuł 21 - Prawo do sprzeciwu
- Artykuł 22 - Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie

## Nowe uprawnienia informacyjne w rodo:

- Informowanie osoby, której dane dotyczą, **przy przekazywaniu danych do państwa trzeciego** lub organizacji międzynarodowej o odpowiednich zabezpieczeniach związanych z przekazaniem.
- Udzielanie informacji o **działaniach podjętych w związku z żądaniem** osoby, której dane dotyczą
- Informowanie o **powodach niepodjęcia działań** w związku z ww. żądaniem oraz o możliwości wniesienia skargi do organu nadzorczego i skorzystania ze środków ochrony prawnej przed sądem
- Informowanie **o naruszeniu ochrony danych** osoby, której one dotyczą, jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić tej osobie podjęcie niezbędnych działań zapobiegawczych
- Informowanie przez organ nadzorczy **o postępach i wynikach rozpatrywania skargi**

## Prawa osoby, której dane dotyczą (Rozdział III)

**Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą (Artykuł 12)**

Administrator podejmuje **odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem** - w szczególności gdy informacje są kierowane do dziecka - udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14, oraz prowadzić z nią wszelką komunikację na mocy art. 15-22 i 34 w sprawie przetwarzania.

Informacji udziela się **na piśmie lub w inny sposób, w tym w stosownych przypadkach - elektronicznie**. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.

## Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą

### **Informacje oraz komunikacja i działania są wolne od**

**opłat.** Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:

- a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo
- b) odmówić podjęcia działań w związku z żądaniem.

**Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.**

## Obowiązek informacyjny (artykuły 13 i 14)

Art. 13 i art. 14 rozporządzenia dzielą informacje udzielane podmiotowi danych na dwie kategorie:

- informacje, których administrator udzielić musi w każdej sytuacji
- informacje, które należy podać, jeżeli są one niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania

*Pojęcie „rzetelności i przejrzystości” jest nieostre - w celu uniknięcia ewentualnych sankcji ze strony organu nadzorczego, administratorzy danych najpewniej będą udzielać najszerszej możliwej informacji.*

## Artykuł 13 Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą

1. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator **podczas pozyskiwania** danych osobowych **podaje jej wszystkie następujące informacje:**
  - a) swoją **tożsamość i dane kontaktowe** oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
  - b) gdy ma to zastosowanie - **dane kontaktowe inspektora ochrony danych;**
  - c) **cele** przetwarzania danych osobowych, oraz **podstawę prawną** przetwarzania;
  - d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) - **prawnie uzasadnione interesy** realizowane przez administratora lub przez stronę trzecią;

## Artykuł 13 Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą

- e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- f) gdy ma to zastosowanie - informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

## Artykuł 13 Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą

2. Poza informacjami, o których mowa w ust. 1, podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, następujące inne **informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:**
- a) **okres, przez który dane osobowe będą przechowywane**, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
  - b) informacje o prawie do żądania od administratora **dostępu do danych** osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
  - c) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) - informacje **o prawie do cofnięcia zgody** w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;



## Artykuł 13 Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą

- d) informacje o **prawie wniesienia skargi** do organu nadzorczego;
- e) informację, **czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy** oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
- f) informacje o **zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu**, o którym mowa w art. 22 ust. 1 i 4, oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

## Artykuł 13 Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą

3. Jeżeli administrator planuje dalej przetwarzać dane osobowe **w celu innym niż cel**, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, **o tym innym celu oraz udziela jej wszelkich innych stosownych informacji**, o których mowa w ust. 2.

### **ZWOLNIENIE!**

4. Ust. 1, 2 i 3 nie mają zastosowania, gdy - i w zakresie, w jakim - osoba, której dane dotyczą, dysponuje już tymi informacjami.

## Artykuł 14 Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą

1. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, administrator **podaje osobie, której dane dotyczą, następujące informacje:**
  - a) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
  - b) gdy ma to zastosowanie - dane kontaktowe inspektora ochrony danych;
  - c) cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania;
  - d) kategorie odnośnych danych osobowych;
  - e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
  - f) gdy ma to zastosowanie - informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

## Artykuł 14 Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą

2. Poza informacjami, o których mowa w ust. 1, administrator podaje osobie, której dane dotyczą, następujące **informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania wobec osoby, której dane dotyczą:**
- a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
  - b) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) - prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
  - c) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

## Artykuł 14 Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą

- d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
- e) informacje o prawie wniesienia skargi do organu nadzorczego;
- f) **źródło pochodzenia danych osobowych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych;**
- g) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

## Artykuł 14 Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą

3. Informacje, o których mowa w ust. 1 i 2, **administrator podaje:**
- a) **w rozsądnym terminie po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca** - mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
  - b) **jeżeli dane osobowe mają być stosowane do komunikacji** z osobą, której dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
  - c) **jeżeli planuje się ujawnić dane osobowe innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu.**

## Artykuł 14 Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą

4. Jeżeli administrator **planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje** on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2.

## Artykuł 14 Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą

### ZWOLNIENIA!

5. Ust. 1- 4 nie mają zastosowania, gdy - i w zakresie, w jakim:

a) osoba, której dane dotyczą, **dysponuje już tymi informacjami**;

b) udzielenie takich informacji okazuje się **niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku**; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1, lub o ile obowiązek, o którym mowa w ust. 1 niniejszego artykułu, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie;



## Artykuł 14 Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą

- c) **pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego,** któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub
- d) **dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej** przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

## **RODO: Artykuł 15 Prawo dostępu przysługujące osobie, której dane dotyczą**

1. **Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia**, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do **uzyskania dostępu do nich oraz następujących informacji**:
  - a) cele przetwarzania;
  - b) kategorie odnośnych danych osobowych;
  - c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
  - d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
  - e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;

## **RODO: Artykuł 15 Prawo dostępu przysługujące osobie, której dane dotyczą**

1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:
  - f) **informacje o prawie wniesienia skargi** do organu nadzorczego;
  - g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą - wszelkie dostępne informacje o ich **źródle**;
  - h) **informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu**, o którym mowa w art. 22 ust. 1 i 4, oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma **prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46, związanych z przekazaniem.**

## **RODO: Prawo dostępu przysługujące osobie, której dane dotyczą**

### **3. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu.**

Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

### **4. Prawo do uzyskania kopii, o której mowa w ust. 3, nie może niekorzystnie wpływać na prawa i wolności innych.**

# RODO: Sprostowanie i usuwanie danych

## Prawo do sprostowania danych (Artykuł 16)

Osoba, której dane dotyczą, ma prawo żądania od administratora **niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe**. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

## **RODO: Prawo do usunięcia danych („prawo do bycia zapomnianym”)**

**Artykuł 17. 1.** Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

- a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
- b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), i nie ma innej podstawy prawnej przetwarzania;
- c) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania;

## **RODO: Prawo do usunięcia danych („prawo do bycia zapomnianym”)**

**Artykuł 17. 1.** Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

- d) dane osobowe były przetwarzane niezgodnie z prawem;
- e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
- f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1.

## RODO: Prawo do usunięcia danych („prawo do bycia zapomnianym”)

**Artykuł 17. 2.** Jeżeli administrator **upublicznił dane osobowe**, a na mocy ust. 1 ma obowiązek usunąć te dane osobowe, to - biorąc pod uwagę dostępną technologię i koszt realizacji - podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.



## **RODO: Prawo do usunięcia danych („prawo do bycia zapomnianym”)**

**Artykuł 17. 3. Ust. 1 i 2 nie mają zastosowania,  
w zakresie w jakim przetwarzanie jest niezbędne:**

- a) do korzystania z prawa do wolności wypowiedzi i informacji;
- b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3;
- d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
- e) do ustalenia, dochodzenia lub obrony roszczeń.

## **RODO: Prawo do ograniczenia przetwarzania**

**Artykuł 18. 1.** Osoba, której dane dotyczą, ma prawo żądania od administratora **ograniczenia przetwarzania** w następujących przypadkach:

- a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych - na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;
- b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
- c) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
- d) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania - do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

## RODO: Prawo do ograniczenia przetwarzania

**Artykuł 18. 2.** Jeżeli na mocy ust. 1 przetwarzanie zostało ograniczone, **takie dane osobowe można przetwarzać, z wyjątkiem przechowywania**, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

**3.** Przed uchyceniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia na mocy ust. 1.

# RODO: Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania

## Artykuł 19

**Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania**, których dokonał zgodnie z art. 16, art. 17 ust. 1 i art. 18, każdego odbiorcę, któremu ujawniono dane osobowe, **chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku**. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

# RODO: Prawo do przenoszenia danych

**Artykuł 20.1.** Osoba, której dane dotyczą, **ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi,** oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli:

- a) przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) lub na podstawie umowy w myśl art. 6 ust. 1 lit. b); oraz
- b) przetwarzanie odbywa się w sposób zautomatyzowany.

## RODO: Prawo do przenoszenia danych

**Artykuł 20. 2.** Wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, **ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.**

3. Wykonanie prawa, o którym mowa w ust. 1 niniejszego artykułu, pozostaje bez uszczerbku dla art. 17. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.
4. Prawo, o którym mowa w ust. 1, nie może niekorzystnie wpływać na prawa i wolności innych.

## RODO: Prawo do sprzeciwu

**Artykuł 21.1.** Osoba, której dane dotyczą, **ma prawo w dowolnym momencie wnieść sprzeciw** - z przyczyn związanych z jej szczególną sytuacją - wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

**2. Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.**

# RODO: Prawo do sprzeciwu

**Artykuł 21.3.** Jeżeli osoba, której dane dotyczą, wnieśli sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.

- 4. Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, o którym mowa w ust. 1 i 2, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.**
5. W związku z korzystaniem z usług społeczeństwa informacyjnego i bez uszczerbku dla dyrektywy 2002/58/WE osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.
6. Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, osoba, której dane dotyczą, ma prawo wnieść sprzeciw - z przyczyn związanych z jej szczególną sytuacją - wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.



# **RODO: Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie**

**Artykuł 22.1.** Osoba, której dane dotyczą, ma prawo do tego, by **nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.**

2. Ust. 1 nie ma zastosowania, jeżeli ta decyzja:

- a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;
- b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
- c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

## **RODO: Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie**

- Artykuł 22. 3.** W przypadkach, o których mowa w ust. 2 lit. a) i c), **administrator wdraża właściwe środki ochrony** praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a **co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.**
- 4.** Decyzje, o których mowa w ust. 2, nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 9 ust. 1, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

## RODO: Ograniczenia

**Artykuł 23. 1.** Prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12-22 i w art. 34, a także w art. 5 - o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12-22 - jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym:

- a) bezpieczeństwu narodowemu;
- b) obronie;
- c) bezpieczeństwu publicznemu;
- d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom;
- e) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu;

# Ograniczenia

## Artykuł 23. 1.

- f) ochronie niezależności sądów i postępowania sądowego;
- g) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu postępowań w takich sprawach, ich wykrywaniu oraz ściganiu;
- h) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a) - e) oraz g);
- i) ochronie osoby, której dane dotyczą, lub praw i wolności innych osób;
- j) egzekucji roszczeń cywilnoprawnych.

## **RODO: Ograniczenia**

**Artykuł 23. 2.** W szczególności akt prawny, o którym mowa w ust. 1, musi zawierać szczegółowe przepisy przynajmniej - w stosownym przypadku - o:

- a) celach przetwarzania lub kategorii przetwarzania;
- b) kategoriach danych osobowych;
- c) zakresie wprowadzonych ograniczeń;
- d) zabezpieczeniach zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu;
- e) określeniu administratora lub kategorii administratorów;
- f) okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania;
- g) ryzyka naruszenia praw lub wolności osoby, której dane dotyczą; oraz
- h) prawie osób, której dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia.

## Ograniczenia/projekt: przepisy wprowadzające uodo

**Art. 52.** W ustawie z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz.U. z 2016 r. poz. 2062, z późn. zm.) wprowadza się następujące zmiany:(...)

**Art.157 § 2b.** Do przetwarzania danych osobowych, o których mowa w § 2a, przepisów **art. 13-15 ust. 1 i 3, 18, 19 i 21** rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) ( Dz. Urz. UE L 119 z 4.05.2016, str. 1), zwane dalej „rozporządzeniem 2016/679”, nie stosuje się.

§ 2c. Wyłączenia, o których mowa w § 2b, stosuje się w przypadku danych osobowych niezbędnych do zapewnienia prawidłowej realizacji zadań, obowiązków lub uprawnień, o których mowa w § 2a.

§ 2d. Przepisu **art. 16** rozporządzenia 2016/679 nie stosuje się, chyba, że przepis szczególny stanowi inaczej.

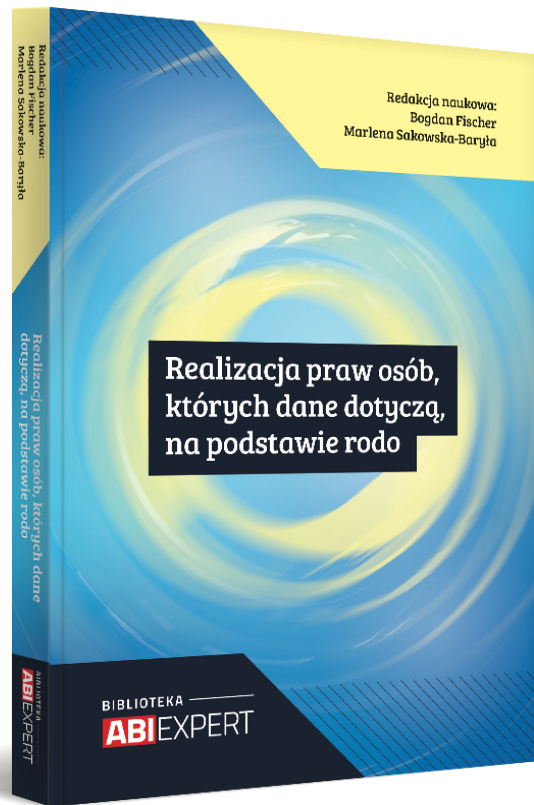
## Ograniczenia/projekt: przepisy wprowadzające uodo

**Art. 168a.** §2. Do przetwarzania danych osobowych, o których mowa w § 1, przepisów **art. 13-15 ust. 1 i 3, 18, 19 i 21** rozporządzenia 2016/679 nie stosuje się.

§3. Wyłączenia, o których mowa w § 2, stosuje się w przypadku danych osobowych niezbędnych do zapewnienia prawidłowej realizacji zadań, obowiązków lub uprawnień, o których mowa w § 1.

§4. Przepisu **art. 16** rozporządzenia 2016/79 nie stosuje się, chyba że przepis szczególny stanowi inaczej. §5. Dane osobowe, o których mowa w § 1, podlegają zabezpieczeniom zapobiegającym nadużyciom i niezgodnemu z prawem dostępowi lub przekazywaniu, wynikającym z procedur prawnych, w których toku są przetwarzane.

**Art. 175f.** Do przetwarzania danych osobowych w postępowaniach sądowych, w rejestrach sądowych albo w sądowych systemach teleinformatycznych, przepisów **art. 13-16 oraz 18-21** rozporządzenia 2016/679 nie stosuje się.



**redakcja naukowa:**

Bogdan Fischer,

Marlena Sakowska-Baryła

**Autorzy:** Aleksandra Błaszczewska, Agnieszka Gryszczyńska, Arleta Nerka, Arwid Mednis, Justyna Kurek, Krzysztof Wygoda, Maciej Kawecki, Marcin Górski, Mariola Więckowska, Mariusz Krzysztofek, Miłosz Mazewski, Mirosław Gumularz, Paweł Fajgielski, Piotr Siemieniak, Urszula Stańczak, Wiesława Kuberska.



# Informowanie o naruszeniach

W kontekście **obowiązku** **notyfikacji** naruszeń zasad przetwarzania danych organowi nadzorczemu i osobom, których dane dotyczą

- weryfikacja procesu obsługi incydentów bezpieczeństwa danych
- należy dostosować Istniejące schematy działania , w tym rozszerzyć o aspekt informowania regulatora oraz osób, których dane zostały dotknięte zdarzeniem, zgodnie z wymaganiami RODO
- dokonujemy przeglądu procedur zarządzania kryzysowego
- konieczne odpowiednie dokumentowanie wykonania tego obowiązku

## RODO: Artykuł 33 Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

1. W przypadku **naruszenia ochrony danych osobowych**, administrator bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie **72 godzin** po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.  
Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się **wyjaśnienie przyczyn opóźnienia**.
2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.

## RODO: Artykuł 33 Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

3. **Zgłoszenie**, o którym mowa w ust. 1, **musi co najmniej**:
- a) **opisywać charakter naruszenia** ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
  - b) **zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych** lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
  - c) **opisywać możliwe konsekwencje** naruszenia ochrony danych osobowych;
  - d) **opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu** ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

## RODO: Artykuł 33 Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

4. Jeżeli - i w zakresie, w jakim - informacji nie da się udzielić w tym samym czasie, można je udzielać **sukcesywnie bez zbędnej zwłoki**
5. **Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych**, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.  
**Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.**

## RODO: Artykuł 34 Zawiadamanie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

1. Jeżeli naruszenie ochrony danych osobowych może powodować **wysokie ryzyko naruszenia praw lub wolności osób fizycznych**, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, **jasnym i prostym językiem** opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d).

## RODO: Artykuł 34 Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

### 3. Zawiadomienie, o którym mowa w ust. 1, **nie jest wymagane**, w następujących przypadkach:

- a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiający odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
  - b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
  - c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.
4. Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy - biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko - może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 3.

# Lista zadań

- **Przegląd procesów globalnych transferów danych**, jeśli takie dotyczą organizacji.
- Konieczny jest także przegląd **procedur\_retencji danych**.

## Wyznaczenie Inspektora Ochrony Danych

### podjęcie działań związanych z wyznaczeniem Inspektora Ochrony Danych (IOD)

- ocena konieczności wyznaczenia IOD,
- administrator i podmiot przetwarzający, którzy nie będą objęci obowiązkiem wyznaczenia IOD, mogą dobrowolnie podjąć decyzję o jego wyznaczeniu.



## Wyznaczenie IOD (obecnie ABI) w rodo

### Artykuł 37. Wyznaczenie inspektora ochrony danych

1. Administrator i podmiot przetwarzający **wyznaczają inspektora ochrony danych, zawsze gdy:**
  - a) **przetwarzania dokonują organ lub podmiot publiczny,** z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
  - b) **główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania,** które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub
  - c) **główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych,** o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

# Administrator/podmiot przetwarzający - organ lub podmiot publiczny

## Projekt z 12.09.2017 r. ustawy o ochronie danych osobowych :

[https://mc.gov.pl/files/ustawa\\_o\\_ochronie\\_danych\\_osobowych\\_-\\_projekt\\_-\\_13.09.2017.pdf](https://mc.gov.pl/files/ustawa_o_ochronie_danych_osobowych_-_projekt_-_13.09.2017.pdf)

**Art. 4.** Przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora, o których mowa w art. 37 ust. 1 lit. a rozporządzenia 2016/679, rozumie się organy publiczne wskazane w art. 5 § 2 pkt 3 Kodeksu postępowania administracyjnego oraz podmioty publiczne wskazane w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, (Dz. U. z 2016 r. poz. 1870, z późn. zm.).

## organ lub podmiot publiczny – projekt ustawy

- **art. 5 § 2 kpa**

3) **organy administracji publicznej** - rozumie się przez to ministrów, centralne organy administracji rządowej, wojewodów, działające w ich lub we własnym imieniu inne terenowe organy administracji rządowej (zespolonej i niezespolonej), organy jednostek samorządu terytorialnego oraz organy i podmioty wymienione w art. 1 pkt 2;

**art. 1.** Kodeks postępowania administracyjnego normuje postępowanie:

- 1) przed organami administracji publicznej w należących do właściwości tych organów sprawach indywidualnych rozstrzyganych w drodze decyzji administracyjnych;
- 2) przed innymi organami państwowymi oraz przed innymi podmiotami, gdy są one powołane z mocy prawa lub na podstawie porozumień do załatwiania spraw określonych w pkt 1; (...)

## **Art. 9 ufp. Sektor finansów publicznych tworzą:**

- 1) organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały;
- 2) jednostki samorządu terytorialnego oraz ich związki;
- 2a) związki metropolitalne;
- 3) jednostki budżetowe;
- 4) samorządowe zakłady budżetowe;
- 5) agencje wykonawcze;
- 6) instytucje gospodarki budżetowej;
- 7) państwowe fundusze celowe;
- 8) Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze oraz Kasa Rolniczego Ubezpieczenia Społecznego i fundusze zarządzane przez Prezesa Kasy Rolniczego Ubezpieczenia Społecznego;
- 9) Narodowy Fundusz Zdrowia;
- 10) samodzielne publiczne zakłady opieki zdrowotnej;
- 11) uczelnie publiczne;
- 12) Polska Akademia Nauk i tworzone przez nią jednostki organizacyjne;
- 13) państwowe i samorządowe instytucje kultury;
- 14) inne państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych, banków i spółek prawa handlowego.

## Artykuł 39 Zadania inspektora ochrony danych

1. Inspektor ochrony danych ma następujące zadania:

- a) **informowanie administratora**, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, **o obowiązkach** spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
- b) **monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych**, w tym podział obowiązków, **działania zwiększające świadomość, szkolenia personelu** uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- c) **udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych** oraz monitorowanie jej wykonania zgodnie z art. 35;
- d) **współpraca z organem nadzorczym**;
- e) **pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem**, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

## Przegląd środków technicznych i organizacyjnych

przegląd stosowanych środków technicznych i organizacyjnych, mających na celu zapewnienie bezpieczeństwa danych oraz dostosowanie lub wzmocnienie tych środków, tam gdzie niezbędne

działania podnoszące świadomość PERSONELU, na wszystkich szczeblach struktury organizacyjnej

Dostosowanie dokumentacji lub opracowanie adekwatnej pozwalającej wykazać zgodność przetwarzania i zabezpieczeń z RODO

**Dziękuję za uwagę!**  
m.sakowskabaryla@kancelariasbc.pl

